

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-030287

(43)Date of publication of application : 29.01.2004

(51)Int.Cl.

G06F 13/00

H04L 12/66

(21)Application number : 2002-186299

(71)Applicant : NTT DATA CORP
CYBER SOLUTIONS INC

(22)Date of filing : 26.06.2002

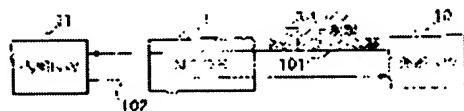
(72)Inventor : KUWATA YOSHITAKA
OTANI HISAMICHI
HOJO TAKESHI
KEENI GLENN MANSFIELD

(54) BI-DIRECTIONAL NETWORK INTRUSION DETECTION SYSTEM AND BI-DIRECTIONAL INTRUSION DETECTION PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a bi-directional network intrusion detection system and a bi-directional intrusion detection program capable of increasing detecting precision by comparing intrusion detection information with a response to intrusion for automatic verification.

SOLUTION: A bi-directional network intrusion detection system(NIDS) 1 monitors an inbound traffic 101 received from an external network(NW) 10, and detects any intrusion and attack. Furthermore, this system 1 monitors an outbound traffic 102 transmitted from an internal network(NW) 11, and detects a response to the detected intrusion. Then, the detected intrusion and a response to this are verified, and when it is determined that the internal network 11 or a host connected to the internal network 11 is influenced, intrusion detection information is outputted.



(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-30287

(P2004-30287A)

(43) 公開日 平成16年1月29日(2004.1.29)

(51) Int.Cl.⁷G06F 13/00
H04L 12/66

F I

G06F 13/00
H04L 12/66351Z
B

テーマコード (参考)

5B089
5K030

審査請求 未請求 請求項の数 7 O L (全 8 頁)

(21) 出願番号 特願2002-186299 (P2002-186299)
(22) 出願日 平成14年6月26日 (2002. 6. 26)(71) 出願人 000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号
(71) 出願人 501175281
株式会社サイバー・ソリューションズ
宮城県仙台市青葉区南吉成六丁目6番地の
3
(74) 代理人 100064908
弁理士 志賀 正武
(74) 代理人 100101465
弁理士 青山 正和
(74) 代理人 100108453
弁理士 村山 靖彦

最終頁に続く

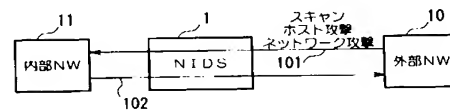
(54) 【発明の名称】 双方向型ネットワーク侵入検知システムおよび双方向型侵入検知プログラム

(57) 【要約】

【課題】 侵入検知情報と侵入に対する応答を比較して自動的に検証し、検知精度を高めることができる双方向型ネットワーク侵入検知システムおよび双方向型侵入検知プログラムを提供する。

【解決手段】 双方向型ネットワーク侵入検知システム（NIDS）1は、外部ネットワーク（NW）10から受信するインバウンドトラフィック101を監視して不正な侵入、攻撃を検知する。さらに、内部ネットワーク（NW）11から発信されるアウトバウンドトラフィック102を監視して検知された不正侵入に対する応答を検出する。そして、検知された不正侵入とそれに対する応答を検証して内部ネットワーク11あるいは内部ネットワーク11に接続されたホストが影響を受けていると判断した場合、侵入検知情報を出力する。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

外部ネットワークから受信されたインバウンドトラフィックを監視してネットワークを介してサーバに侵入する不正侵入を検知する侵入検知手段と、
内部ネットワークから発信されたアウトバウンドトラフィックを監視して不正侵入に対する応答を検出する応答検出手段と、
前記侵入検知手段から出力された検知情報と、前記応答検出手段により検出された応答信号を照合して検証し、不正侵入検知情報を出力する検知情報出力手段と、
を具備することを特徴とする双方向型ネットワーク侵入検知システム。

【請求項 2】

前記検知情報出力手段は、不正侵入を検知後、予め定めた時間内に不正侵入に対する応答が返されていることを判断して、不正侵入検知情報を出力することを特徴とする請求項 1 に記載の双方向型ネットワーク侵入検知システム。

【請求項 3】

前記検知情報出力手段は、前記侵入検知手段により内部ネットワークに接続されたホストに対する侵入が検知された場合、攻撃対象のホストに問い合わせ、該ホストからの応答に異常がある場合、または該ホストから予め定められた時間内に応答がない場合、不正侵入検知情報を出力することを特徴とする請求項 1 に記載の双方向型ネットワーク侵入検知システム。

【請求項 4】

内部ネットワークに接続されたホストは、さらに、侵入検知エージェントを備え、前記検知情報出力手段は、検知した不正侵入を攻撃対象のホストの侵入検知エージェントから取得した検知情報により検証して、不正侵入検知情報を出力することを特徴とする請求項 1 に記載の双方向型ネットワーク侵入検知システム。

【請求項 5】

請求項 1 に記載の双方向型ネットワーク侵入検知システムに、
内部ネットワークに接続されたホストと接続する監視制御ネットワークを備え、ホストの監視制御に用いることを特徴とする双方向型ネットワーク侵入検知システム。

【請求項 6】

外部ネットワークから受信されたインバウンドトラフィックを監視して不正侵入を検知する侵入検知手段と、内部ネットワークから発信されたアウトバウンドトラフィックを監視して不正侵入に対する応答を検出する応答検出手段と、前記侵入検知手段から出力された検知情報と、前記応答検出手段により検出された応答信号を照合して検証し、不正侵入検知情報を出力する検知情報出力手段と、内部ネットワークの通信の異常を検出する通信異常検出手段とを備える侵入検知装置と、
内部ネットワークの運用状態を集中監視し、前記侵入検知装置に内部ネットワークの通信量に関する情報を出力するネットワーク監視制御装置と、
を具備することを特徴とする双方向型ネットワーク侵入検知システム。

【請求項 7】

侵入検知装置によりインバウンドトラフィックを監視して不正侵入を検知するステップと、
前記侵入検知装置によりアウトバウンドトラフィックを監視して検知された不正侵入に対する応答を検出するステップと、
ネットワーク監視制御装置から通信量の情報を受けて通信の異常を検出するステップと、
予め定めた時間内に検知された不正侵入に対する応答が返されていることが検出された場合、あるいは前記通信量に異常が発生した場合、検知された不正侵入検知情報を出力するステップと、
をコンピュータに実行させるための双方向型侵入検知プログラム。

【発明の詳細な説明】

【0001】

10

20

30

40

50

【発明の属する技術分野】

この発明は、コンピュータネットワークにおける不正な手段による侵入を検知し、不正侵入検知情報を出力する侵入検知システムに用いて好適な双方向型ネットワーク侵入検知システムおよび双方向型侵入検知プログラムに関する。

【0002】**【従来の技術】**

各種の情報を提供するWebサーバや電子メールの送受信を行うメールサーバなどネットワークに接続されたコンピュータシステムは、常に不正な侵入や攻撃の危険にさらされている。不正な侵入、攻撃は、必ず侵入前に必要な情報を収集する過程を経て行われる。情報の収集には、ホストの脆弱性を調べるポートスキャンや稼動するアプリケーションの情報を含むバナー情報の入手のためのアクセスなどがある。このような方法によって得られた情報を利用して、コンピュータシステムの脆弱な部分であるセキュリティホールなどを狙い、侵入する。このような攻撃からシステムを防御するために、防御の構成に応じてネットワークやホストを監視する侵入検知システム、ゲートウェイにファイアウォールなどが設けられる。

10

【0003】

従来、ネットワーク型侵入検知システムは、監視するネットワークのインバウンドの信号を監視してパケット情報を検出し、予め設定したルールやシグネチャと比較して不正なアクセスを検知する。そして、侵入検知情報を生成し、出力する。この場合、攻撃の可能性のある侵入に対しては全て不正侵入のアラートが出力される。出力されたアラートの履歴調査、アラートとその侵入に対する影響の検証作業などは、主として手作業で行われる。

20

【0004】**【発明が解決しようとする課題】**

上述のように、従来のネットワーク型侵入検知システムにおいては、監視対象のセグメントまたはホストへのアクセスを監視し、攻撃の可能性のある侵入に対しては全てアラートを出力している。従って、実際にはホストやネットワークに影響を与えないアクセスに対するアラートも多く含まれており、誤検出が多いという問題があった。また、不正侵入を検知するために設定されるルールやシグネチャは非常に多く、これらの情報に基づいて攻撃可能性のある侵入に対して全て検知結果を出力するため、多量のアラートが生成される。そのために、出力されたアラートから本当に危険性の高い攻撃を選択して適切な防御策を迅速に講じることは難しく、検知結果を有効に利用できないという問題があった。

30

【0005】

この発明は、上記の点に鑑みてなされたもので、その目的は、外部ネットワークを監視して検知された侵入検知情報と内部ネットワークを監視して検出した侵入に対する応答信号を比較することによって、攻撃の影響を確認し、実際に影響が確認された侵入の検知情報を不正侵入検知情報として出力するようにして検知精度を高めることができる双方向型ネットワーク侵入検知システムおよび双方向型侵入検知方法並びに双方向型侵入検知プログラムを提供することにある。また、他の目的は、不正侵入に対して、どのような応答が返されているか調べることによって不正侵入の影響を自動的に検証できる双方向型ネットワーク侵入検知システムおよび双方向型侵入検知プログラムを提供することにある。

40

【0006】**【課題を解決するための手段】**

上記の課題を解決するために、請求項1に記載の発明は、外部ネットワークから受信されたインバウンドトラフィックを監視してネットワークを介してサーバに侵入する不正侵入を検知する侵入検知手段と、内部ネットワークから発信されたアウトバウンドトラフィックを監視して不正侵入に対する応答を検出する応答検出手段と、前記侵入検知手段から出力された検知情報と、前記応答検出手段により検出された応答信号を照合して検証し、不正侵入検知情報を出力する検知情報出力手段とを具備することを特徴とする双方向型ネットワーク侵入検知システムである。

【0007】

50

また、請求項2に記載の発明は、請求項1に記載の双方向型ネットワーク侵入検知システムにおいて、前記検知情報出力手段は、不正侵入を検知後、予め定めた時間内に不正侵入に対する応答が返されていることを判断して、不正侵入検知情報を出力することを特徴とする。

【0008】

また、請求項3に記載の発明は、請求項1に記載の双方向型ネットワーク侵入検知システムにおいて、前記検知情報出力手段は、前記侵入検知手段により内部ネットワークに接続されたホストに対する侵入が検知された場合、当該ホストに問い合わせ、該ホストからの応答に異常がある場合、または該ホストから予め定められた時間内に応答がない場合、不正侵入検知情報を出力することを特徴とする。

10

【0009】

また、請求項4に記載の発明は、請求項1に記載の双方向型ネットワーク侵入検知システムにおいて、内部ネットワークに接続されたホストは、さらに、侵入検知エージェントを備え、前記検知情報出力手段は、検知した不正侵入を攻撃対象のホストの侵入検知エージェントから取得した検知情報により検証して、不正侵入検知情報を出力することを特徴とする。

【0010】

また、請求項5に記載の発明は、請求項1に記載の双方向型ネットワーク侵入検知システムに、内部ネットワークに接続されたホストと接続する監視制御ネットワークを備え、ホストの監視制御に用いることを特徴とする双方向型ネットワーク侵入検知システムである。

20

【0011】

また、請求項6に記載の発明は、外部ネットワークから受信されたインバウンドトラフィックを監視して不正侵入を検知する侵入検知手段と、内部ネットワークから発信されたアウトバウンドトラフィックを監視して不正侵入に対する応答を検出する応答検出手段と、前記侵入検知手段から出力された検知情報と、前記応答検出手段により検出された応答信号を照合して検証し、不正侵入検知情報を出力する検知情報出力手段と、内部ネットワークの通信の異常を検出する通信異常検出手段とを備える侵入検知装置と、内部ネットワークの運用状態を集中監視し、前記侵入検知装置に内部ネットワークの通信量に関する情報を出力するネットワーク監視制御装置とを具備することを特徴とする双方向型ネットワーク侵入検知システムである。

30

【0012】

また、請求項7に記載の発明は、侵入検知装置がインバウンドトラフィックを監視して不正侵入を検知するステップと、前記侵入検知装置がアウトバウンドトラフィックを監視して検知された不正侵入に対応する応答を検出するステップと、前記侵入検知装置がネットワーク監視制御装置から通信量の情報を受けて通信の異常を検出するステップと、予め定めた時間内に検知された不正侵入に関係する応答通信が検出された場合、あるいは前記通信量に異常が発生したと判定された場合、検知された不正侵入検知情報を出力するステップとをコンピュータに実行させるための双方向型侵入検知プログラムである。

【0013】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して説明する。図1は、同実施形態による双方向型ネットワーク侵入検知システムの概念図である。同図において、1は、双方向型ネットワーク侵入検知システム（NIDS）であり、外部ネットワーク（NW）10から受信するインバウンドトラフィック101を監視して不正な侵入、攻撃を検知する。不正な侵入、攻撃には、TCPのポートスキャンやUDPのポートスキャンなどのスキャン、内部ネットワークに接続されたホストへの攻撃、TCPのサービスをターゲットとするLandなどのネットワーク攻撃が考えられる。また、双方向型ネットワーク侵入検知システム1は、内部ネットワーク（NW）11から発信されるアウトバウンドトラフィック102を監視して検知された不正侵入に対する応答を検出する。そして、検知された不正侵

40

50

入とそれに対する応答を検証して内部ネットワーク 11 あるいは内部ネットワーク 11 に接続されたホストが影響を受けていると判断した場合、侵入検知情報を出力する。この出力は、ログとして記録され、さらに、内部ネットワーク 11 の管理者に対してメールなどのアラート発生通知が送られる。また、アウトバウンドトラフィックに影響を与えなかった攻撃に関しても、後の解析のために未然の攻撃としてログに記録することができる。

【0014】

図 2 は、双方向型ネットワーク侵入検知システム 1 の構成を示すブロック図である。2 は、外部ネットワーク 10 から受信されたパケットを監視することによる不正侵入の検知、内部ネットワーク 11 の監視による不正侵入に対する応答の検出および不正侵入検知情報と応答の比較、検証を行う侵入検知装置である。不正侵入の検知は、インバウンドトラフィック 101 のプロトコルのパケット内容を解析し、予めデータベースに設定されたルールおよび不正な通信の情報から成るシグネチャと比較して行われる。

10

【0015】

3 は、内部ネットワーク 11 とホスト 20-1 ~ 4 の監視制御を行うネットワーク監視制御装置であり、侵入検知装置 2 にトラフィック量に関する情報を供給する。このネットワーク監視制御装置 3 内には数分間のアウトバウンドトラフィックを記録する循環バッファ（サイクリックバッファ、リングバッファ）が設けられている。ここで、循環バッファとは、一定サイズのメモリであり、Full 状態になった場合に最も古いデータから順次消去されて新しいデータが書き込まれる。4 は、外部ネットワーク 10 と内部ネットワーク 11 を相互接続するゲートウェイ（GW）である。GW はパケットをその通信内容によってフィルタリングするファイヤウォール（FW）の機能を持つことも可能である。内部ネットワーク 11 に接続されたホスト 20-1 ~ 4 は、監視エージェントと侵入検知エージェントを備える。

20

【0016】

以下、図 1 および図 2 を参照して、双方向型ネットワーク侵入検知システム 1 の動作を説明する。まず、外部ネットワーク 10 からの侵入は、侵入検知装置 2 によって検知される。侵入検知装置 2 は、この検知した不正侵入の種類によって次の 3 つの手順に分けて検知情報の照合、検証を行う。（1）ポートスキャンの場合：内部ネットワーク 11 に接続されたホスト 20-1 ~ 4 のいずれかをターゲットとしたポートスキャン、例えば、当該ホストの各ポートに対して、コネクションを確立できるかどうか試みてホストで稼動しているサービスを調べるスキャンなどが検知された場合、アウトバウンド 102 の通信を監視してポートスキャンに対する応答を調べる。一定の時間内に応答が返されているとき、あるいは誤った応答が返されている場合、例えば、smtp（Simple Mail Transfer Protocol）ポートへのスキャンを検知した後、メールサーバではないホストから応答が返されている場合など、不正侵入と判断して侵入検知情報を出力する。一方、一定の時間内に応答がない場合、アラートは生成されず、ホスト 20-1 ~ 4 に影響を与えなかった未然の侵入として侵入検知装置 2 の記憶装置に記憶される。

30

【0017】

（2）ホストへの攻撃の場合：ホスト 20-1 ~ 4 のいずれかに対する攻撃、例えば、サービスをダウンさせる攻撃、過負荷状態にして利用できなくする攻撃などが検知された場合、攻撃対象のホストから一定の時間内に応答が返されているか否か調べる。応答が返されているとき、侵入検知装置 2 は、攻撃対象のホストの監視エージェントおよび侵入検知エージェントに問い合わせを行う。当該監視エージェントから応答がない場合、あるいは侵入検知エージェントから検知情報が出力されている場合、ホストへの有効な攻撃と判断して、侵入検知情報を出力する。また、ホストの特権ユーザ権取得の試みが検知された後、当該エージェントから特権ユーザのログインが確認された場合もホストへの有効な攻撃と判断する。

40

【0018】

（3）ネットワークへの攻撃の場合：この種の攻撃として、特殊なパケットを攻撃対象のホストに送りフリーズさせてしまう Land、トラフィックを過負荷状態にする攻撃など

50

がある。侵入検知装置 2 は、このような内部ネットワーク 11 への攻撃を検知した場合、ネットワーク監視制御装置 3 にトラフィック量を問い合わせる。そして、ネットワーク監視制御装置 3 から通知されたトラフィック量に基づいて、トラフィック量あるいはトラフィック量の変化が予め定めたしきい値を越えているか否か判断し、しきい値より大きい場合、攻撃により発生したトラフィックの異常と判断して検知情報を出力する。

【0019】

図 3 は、侵入検知装置 2、ネットワーク監視制御装置 3、ホスト 20-1~4 のエージェントを接続する監視制御用ネットワーク 5 を設けた双方向型侵入検知ネットワークの構成を示す図である。監視制御用ネットワーク 5 を用いて侵入検知装置 2 とネットワーク監視制御装置 3 間の通信およびエージェントの監視制御を行うことができるので、内部ネットワーク 11 のトラフィックの状態に影響されない侵入検知システムを構築できる。

10

なお、侵入検知エージェントからの検出信号が無くても、アウトバウンドトラフィック（通信）の種類と量の異常のみで、不正アクセスを検知してもよい。

【0020】

【発明の効果】

以上説明したように、本発明によれば、侵入検知装置によって検知された不正侵入を、当該不正侵入に対する応答と照合してその影響を調べて実際に影響を受けている侵入のみを検知情報として出力するので、侵入検知精度が高くなり、効果的な防御策を施すことができるという効果が得られる。また、不正侵入の検知情報を、侵入に対する応答と照合することによって自動的に検証し、選択するので、出力されるアラート数は大幅に削減され、侵入履歴の調査や侵入の検証作業を効率化できるという効果が得られる。

20

【図面の簡単な説明】

【図 1】本発明の一実施の形態による双方向型ネットワーク侵入検知システムを示す概念図である。

【図 2】同実施形態の双方向型ネットワーク侵入検知システムの構成を示すブロック図である。

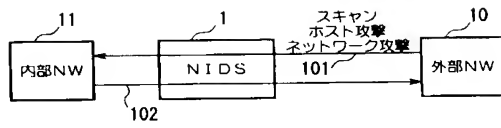
【図 3】図 2 の双方向型ネットワーク侵入検知システムに監視制御用ネットワークを付加した構成を示すブロック図である。

【符号の説明】

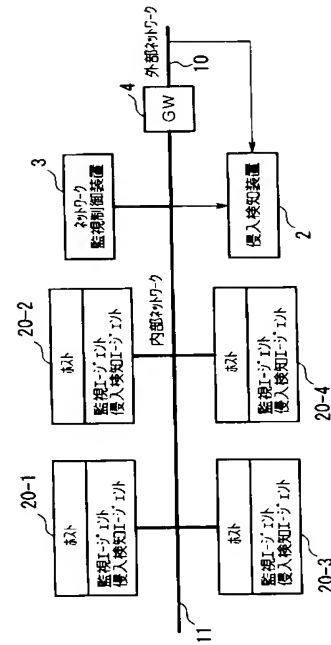
- 1 双方向型ネットワーク侵入検知装置（NIDS）
- 2 侵入検知装置
- 3 ネットワーク監視制御装置
- 4 ゲートウェイ（GW）
- 5 監視制御用ネットワーク

30

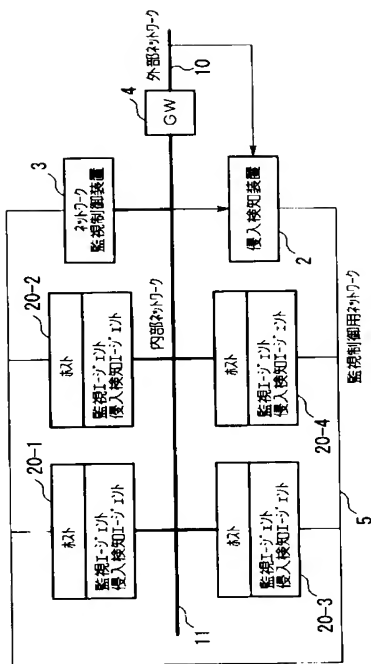
【図 1】



【図 2】



【図 3】



フロントページの続き

(72)発明者 桑田 喜隆

東京都江東区豊洲三丁目3番3号 株式会社エヌ・ティ・ティ・データ内

(72)発明者 大谷 尚通

東京都江東区豊洲三丁目3番3号 株式会社エヌ・ティ・ティ・データ内

(72)発明者 北條 武

東京都江東区豊洲三丁目3番3号 株式会社エヌ・ティ・ティ・データ内

(72)発明者 キニ グレン マンスフィールド

宮城県仙台市青葉区南吉成六丁目6番地の3 株式会社サイバー・ソリューションズ内

Fターム(参考) 5B089 GA04 GB02 KA17

5K030 GA15 HC01 HC13 HD03 HD06